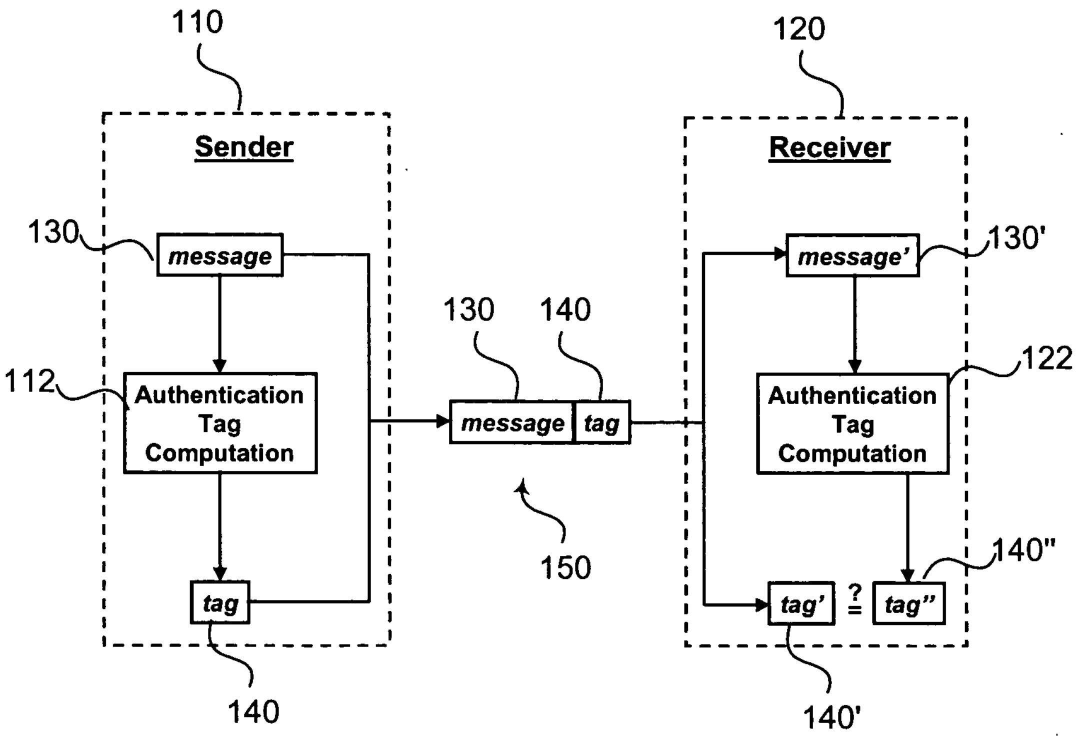

110
Sender
130
message
112
Authentication Tag Computation
tag
140
130
140
message
tag
150
120
Receiver
message'
130'
122
Authentication Tag Computation
tag'
?
=
tag"
140"
140'

FIG. 1

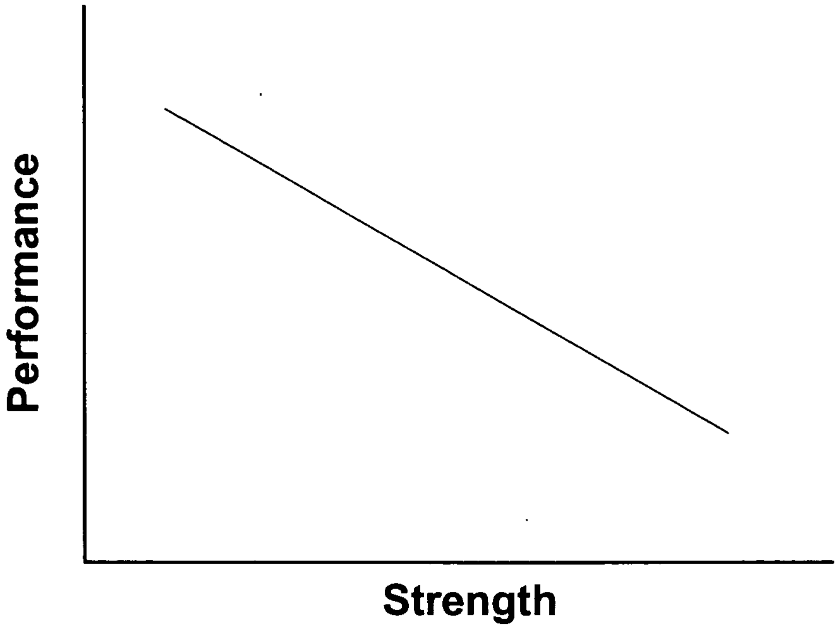


FIG. 2

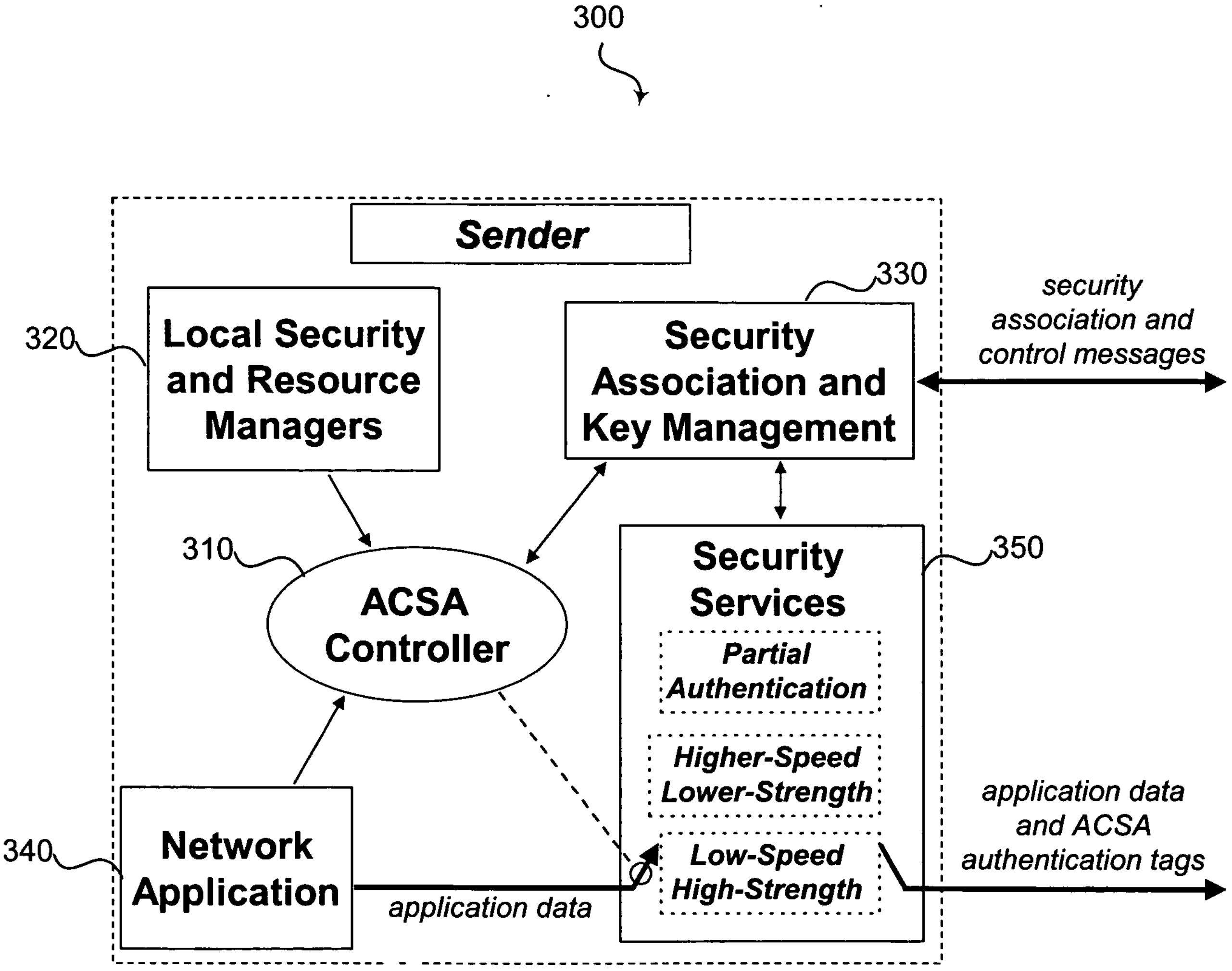

300
Sender
320
Local Security and Resource Managers
330
Security Association and Key Management
security association and control messages
310
ACSA Controller
350
Security Services
Partial Authentication
Higher-Speed Lower-Strength
Low-Speed High-Strength
340
Network Application
application data
application data and ACSA authentication tags

FIG. 3

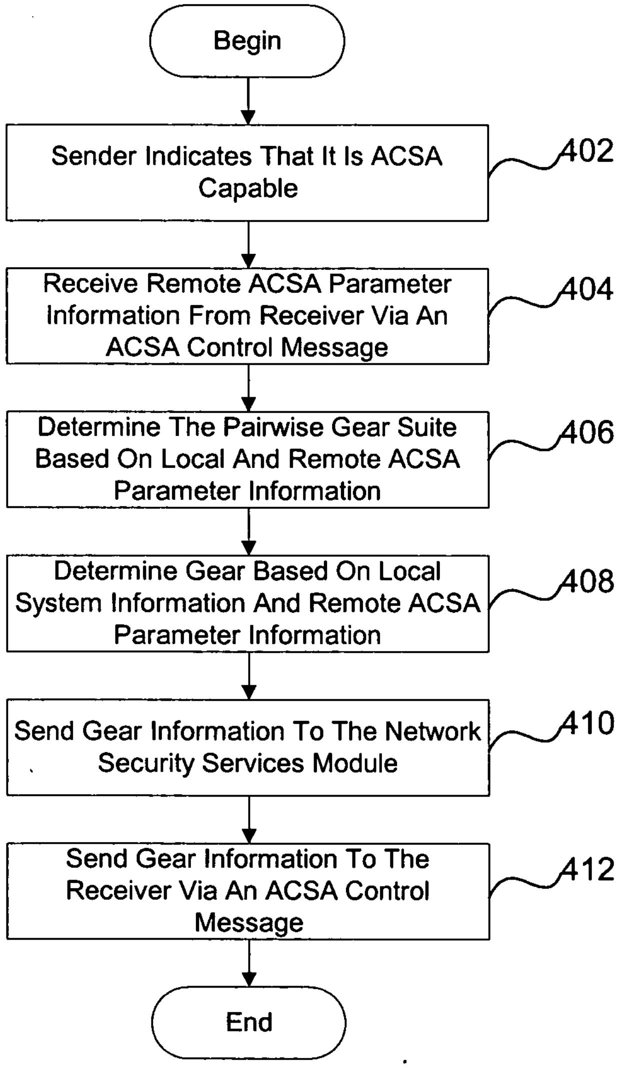

Begin
Sender Indicates That It Is ACSA Capable
402
Receive Remote ACSA Parameter Information From Receiver Via An ACSA Control Message
404
Determine The Pairwise Gear Suite Based On Local And Remote ACSA Parameter Information
406
Determine Gear Based On Local System Information And Remote ACSA Parameter Information
408
Send Gear Information To The Network Security Services Module
410
Send Gear Information To The Receiver Via An ACSA Control Message
412
End

FIG. 4

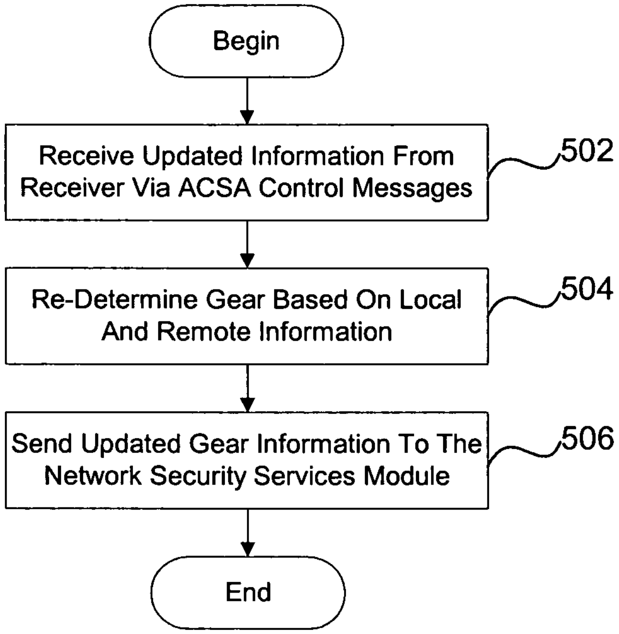

Begin
Receive Updated Information From Receiver Via ACSA Control Messages
502
Re-Determine Gear Based On Local And Remote Information
504
Send Updated Gear Information To The Network Security Services Module
506
End

FIG. 5

		Receiver Processor Utilization		
		Too Heavily Loaded	Near Desired CPU Load	Lightly Loaded
Sender Processor Utilization	Too Heavily Loaded	switch to less computationally intensive gear	switch to less computationally intensive gear	switch to less computationally intensive gear
	Near Desired CPU Load	switch to less computationally intensive gear	maintain current gear	maintain current gear
	Lightly Loaded	switch to less computationally intensive gear	maintain current gear	switch to more secure (more computationally intensive) gear

FIG. 6

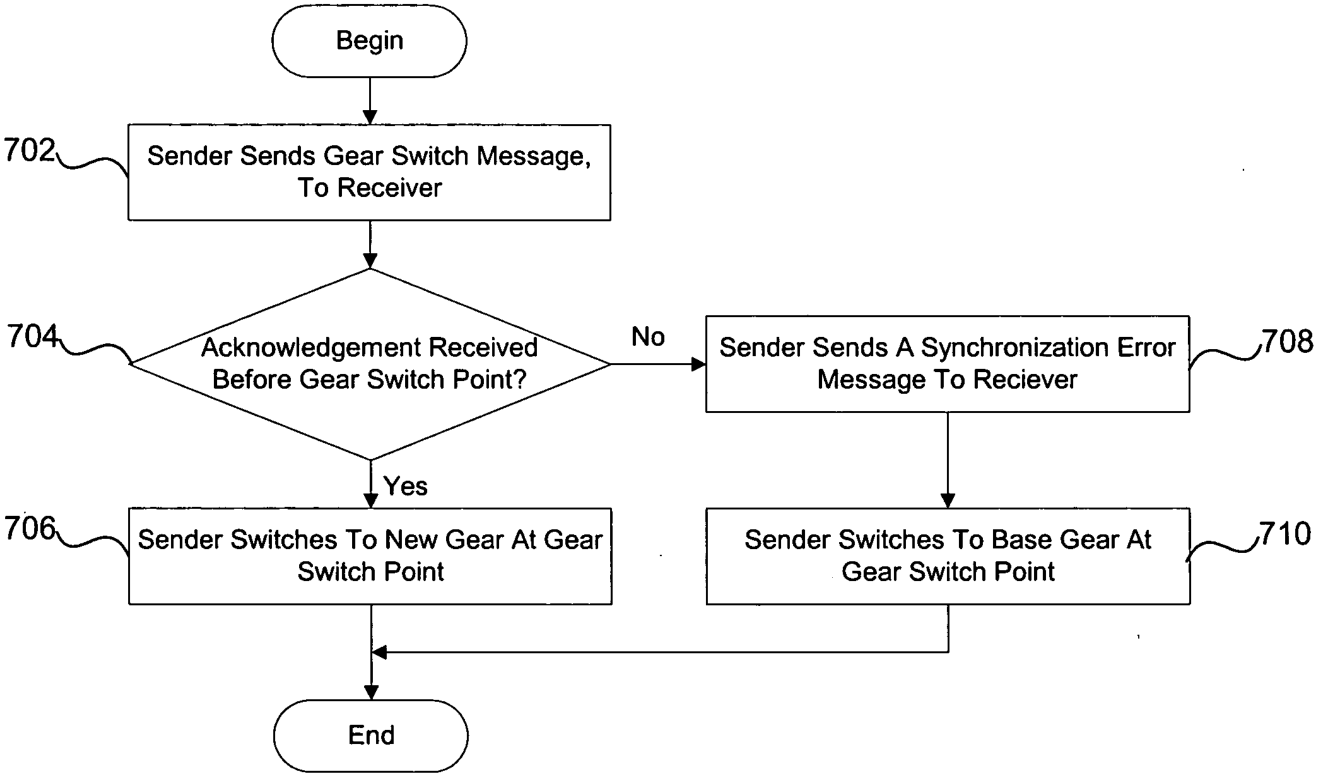

Begin
702
Sender Sends Gear Switch Message, To Receiver
704
Acknowledgement Received Before Gear Switch Point?
No
708
Sender Sends A Synchronization Error Message To Reciever
Yes
706
Sender Switches To New Gear At Gear Switch Point
710
Sender Switches To Base Gear At Gear Switch Point
End

FIG. 7A

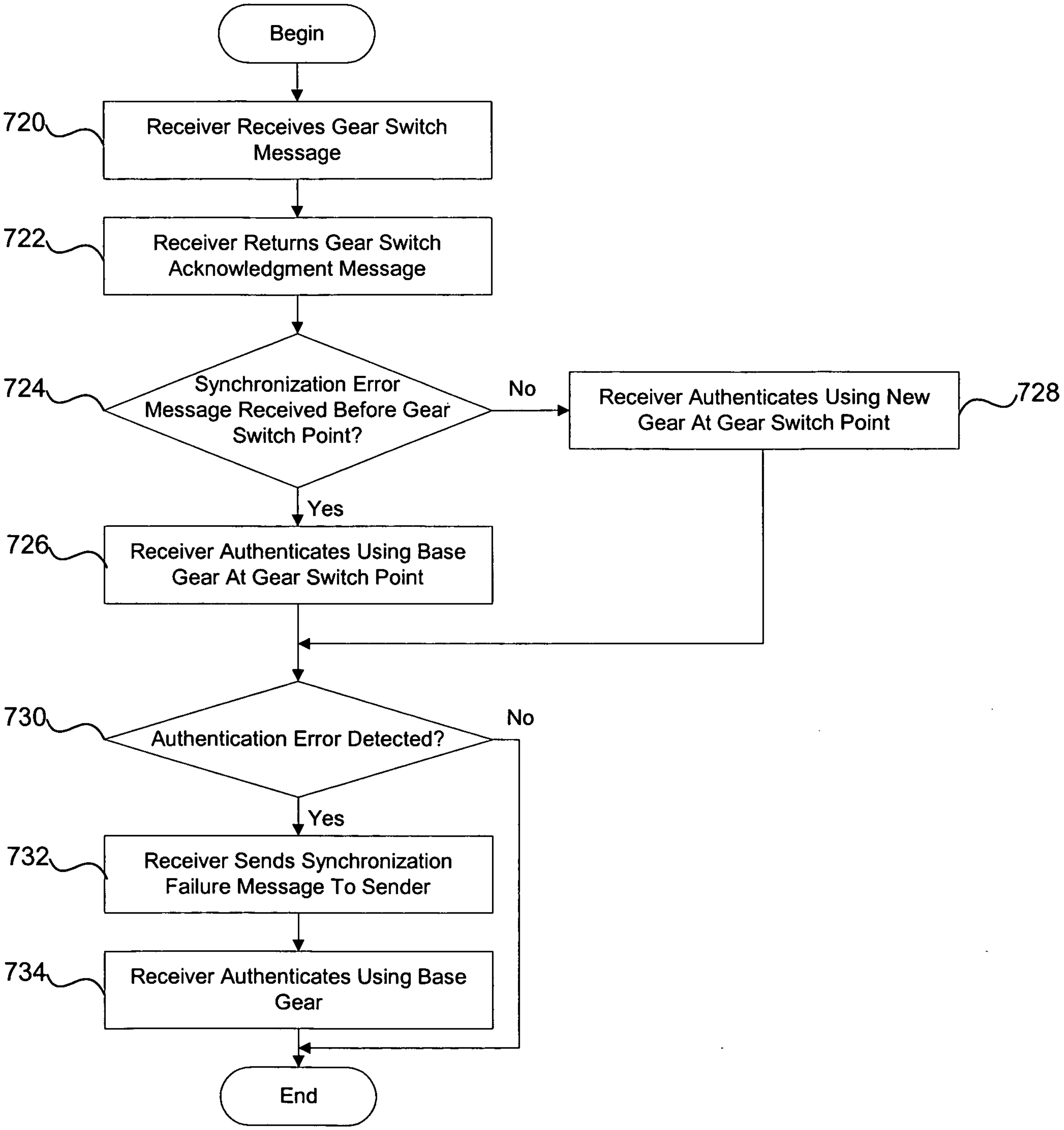
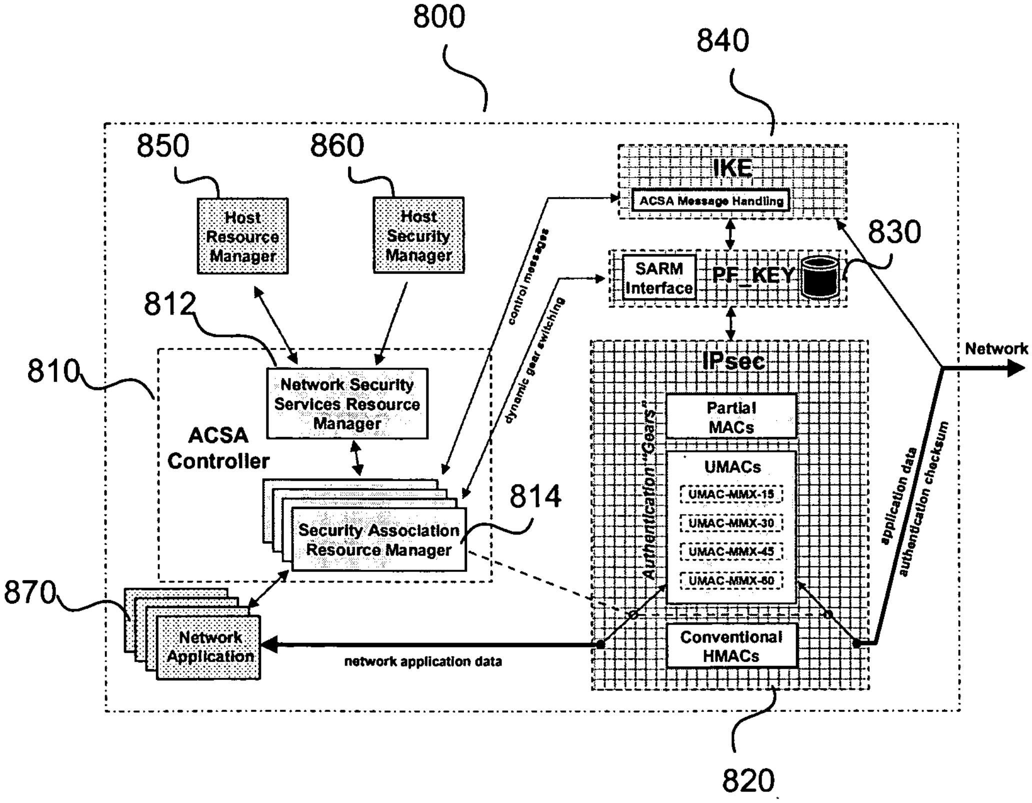

Begin
720
Receiver Receives Gear Switch Message
722
Receiver Returns Gear Switch Acknowledgment Message
724
Synchronization Error Message Received Before Gear Switch Point?
No
Receiver Authenticates Using New Gear At Gear Switch Point
728
Yes
726
Receiver Authenticates Using Base Gear At Gear Switch Point
730
Authentication Error Detected?
No
Yes
732
Receiver Sends Synchronization Failure Message To Sender
734
Receiver Authenticates Using Base Gear
End

FIG. 7B



800
840
IKE
ACSA Message Handling
850
860
Host Resource Manager
Host Security Manager
830
SARM Interface
PF_KEY
control messages
dynamic gear switching
812
810
Network Security Services Resource Manager
ACSA Controller
IPsec
Network
Partial MACs
UMACs
UMAC-MMX-15
UMAC-MMX-30
UMAC-MMX-45
UMAC-MMX-60
Authentication "Gears"
814
Security Association Resource Manager
application data
authentication checksum
870
Network Application
network application data
Conventional HMACs
820

FIG. 8

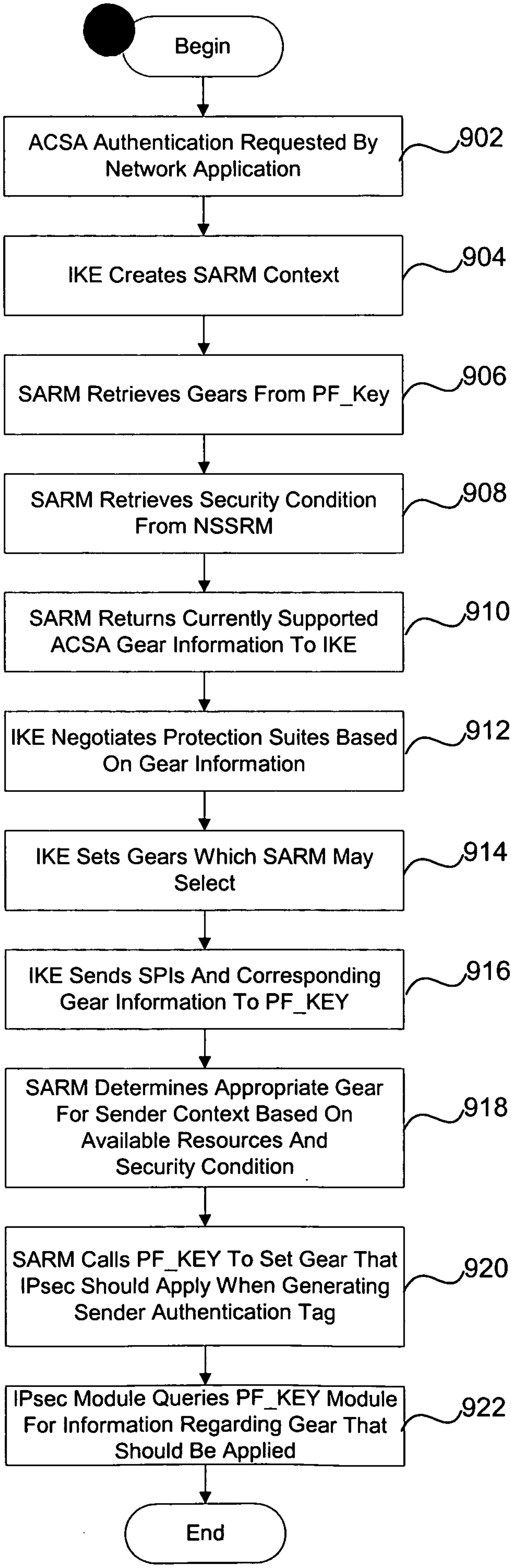

Begin
ACSA Authentication Requested By Network Application
902
IKE Creates SARM Context
904
SARM Retrieves Gears From PF_Key
906
SARM Retrieves Security Condition From NSSRM
908
SARM Returns Currently Supported ACSA Gear Information To IKE
910
IKE Negotiates Protection Suites Based On Gear Information
912
IKE Sets Gears Which SARM May Select
914
IKE Sends SPIs And Corresponding Gear Information To PF_KEY
916
SARM Determines Appropriate Gear For Sender Context Based On Available Resources And Security Condition
918
SARM Calls PF_KEY To Set Gear That IPsec Should Apply When Generating Sender Authentication Tag
920
IPsec Module Queries PF_KEY Module For Information Regarding Gear That Should Be Applied
922
End

FIG. 9

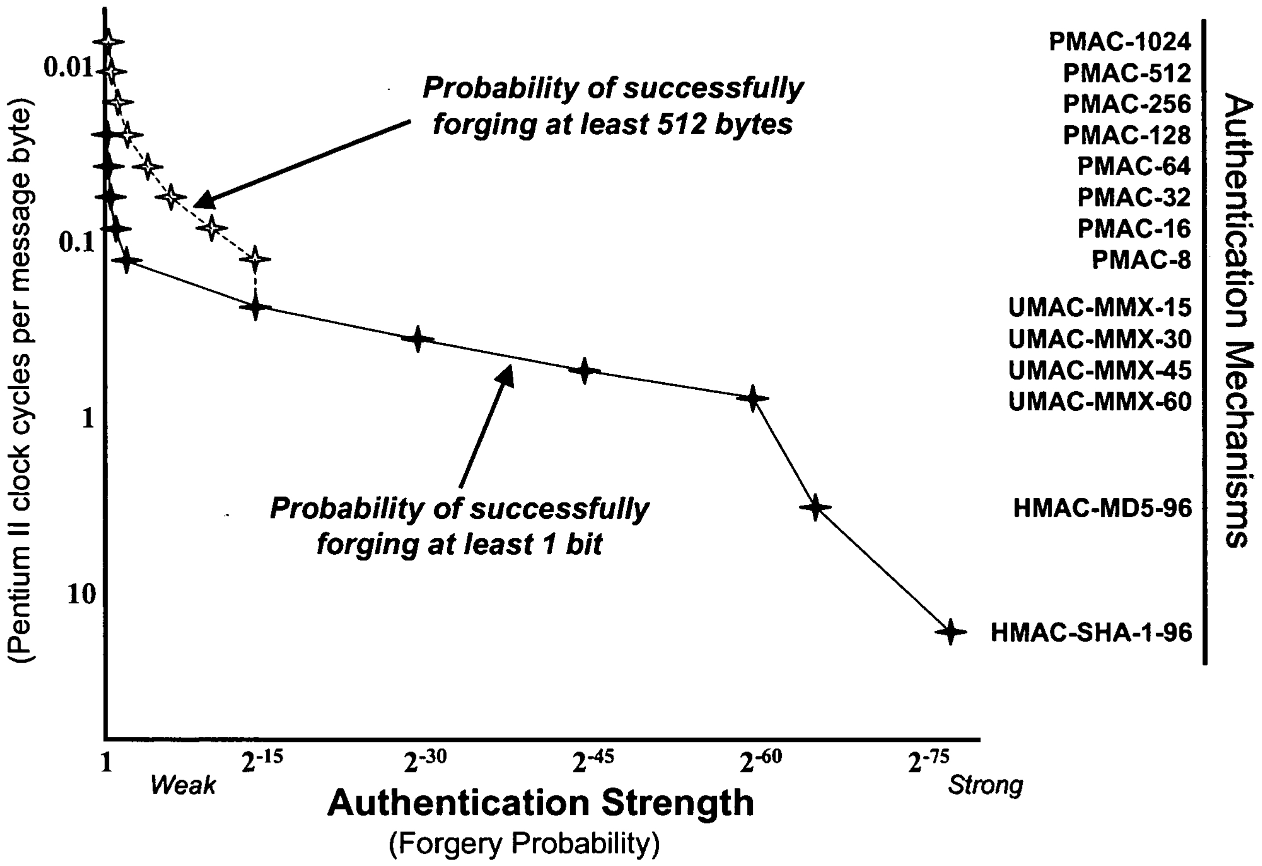

0.01
0.1
1
10
Performance
(Pentium II clock cycles per message byte)
1
2-15
2-30
2-45
2-60
2-75
Weak
Strong
Authentication Strength
(Forgery Probability)
Probability of successfully forging at least 512 bytes
Probability of successfully forging at least 1 bit
PMAC-1024
PMAC-512
PMAC-256
PMAC-128
PMAC-64
PMAC-32
PMAC-16
PMAC-8
UMAC-MMX-15
UMAC-MMX-30
UMAC-MMX-45
UMAC-MMX-60
HMAC-MD5-96
HMAC-SHA-1-96
Authentication Mechanisms

FIG. 10

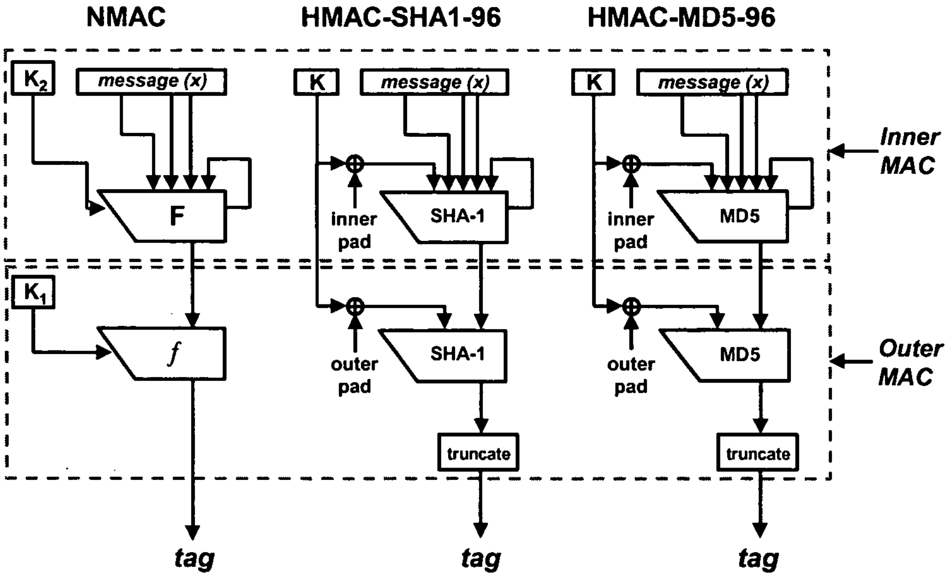

NMAC
HMAC-SHA1-96
HMAC-MD5-96
K2
message (x)
F
K1
f
K
message (x)
inner pad
SHA-1
outer pad
SHA-1
truncate
K
message (x)
inner pad
MD5
outer pad
MD5
truncate
Inner MAC
Outer MAC
tag
tag
tag

FIG. 11

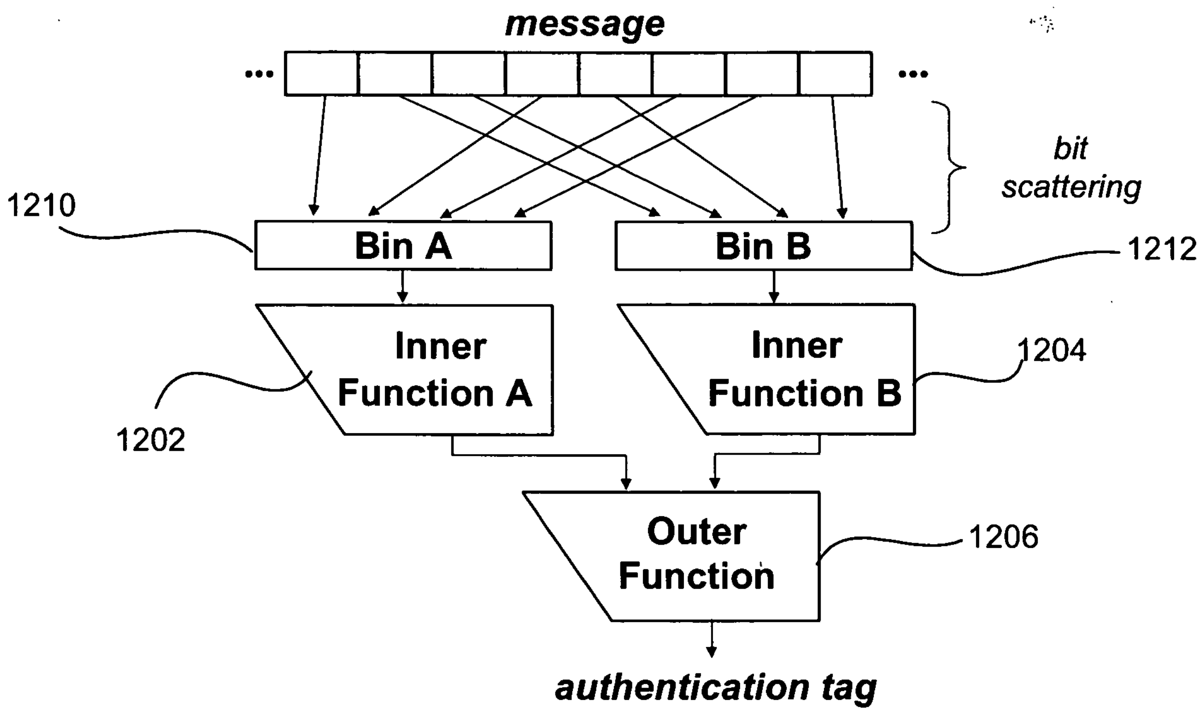

message
...
...
bit scattering
1210
Bin A
Bin B
1212
Inner Function A
Inner Function B
1204
1202
Outer Function
1206
authentication tag

FIG. 12

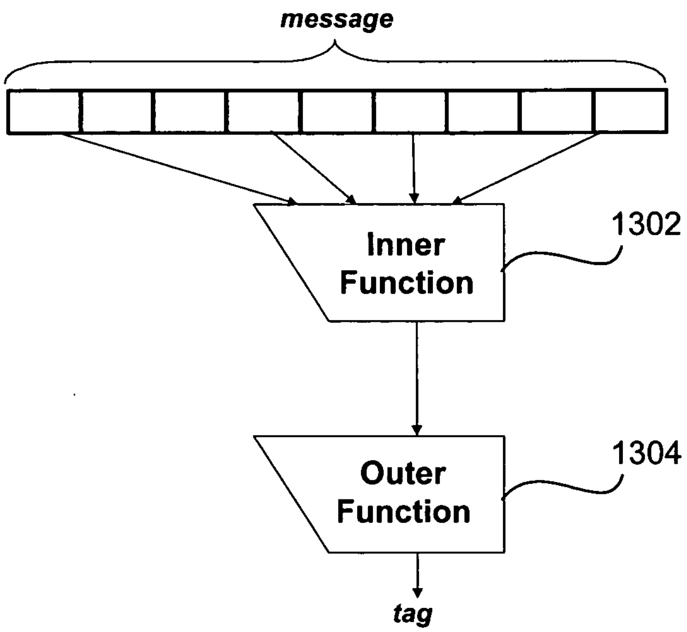


FIG. 13

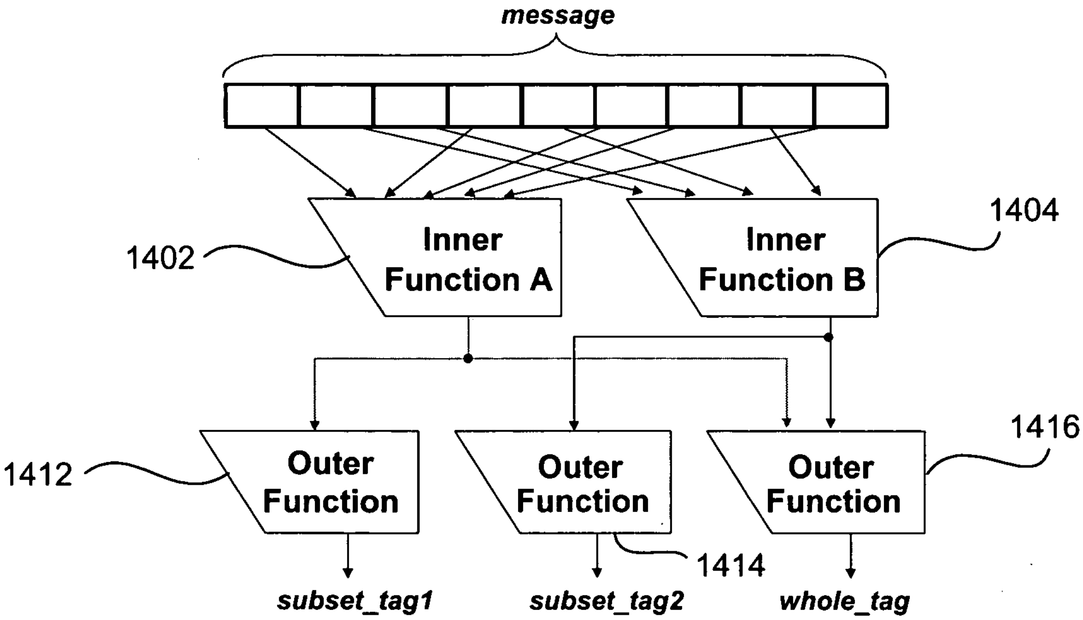

message
Inner Function A
Inner Function B
1402
1404
Outer Function
Outer Function
Outer Function
1412
1414
1416
subset_tag1
subset_tag2
whole_tag

FIG. 14

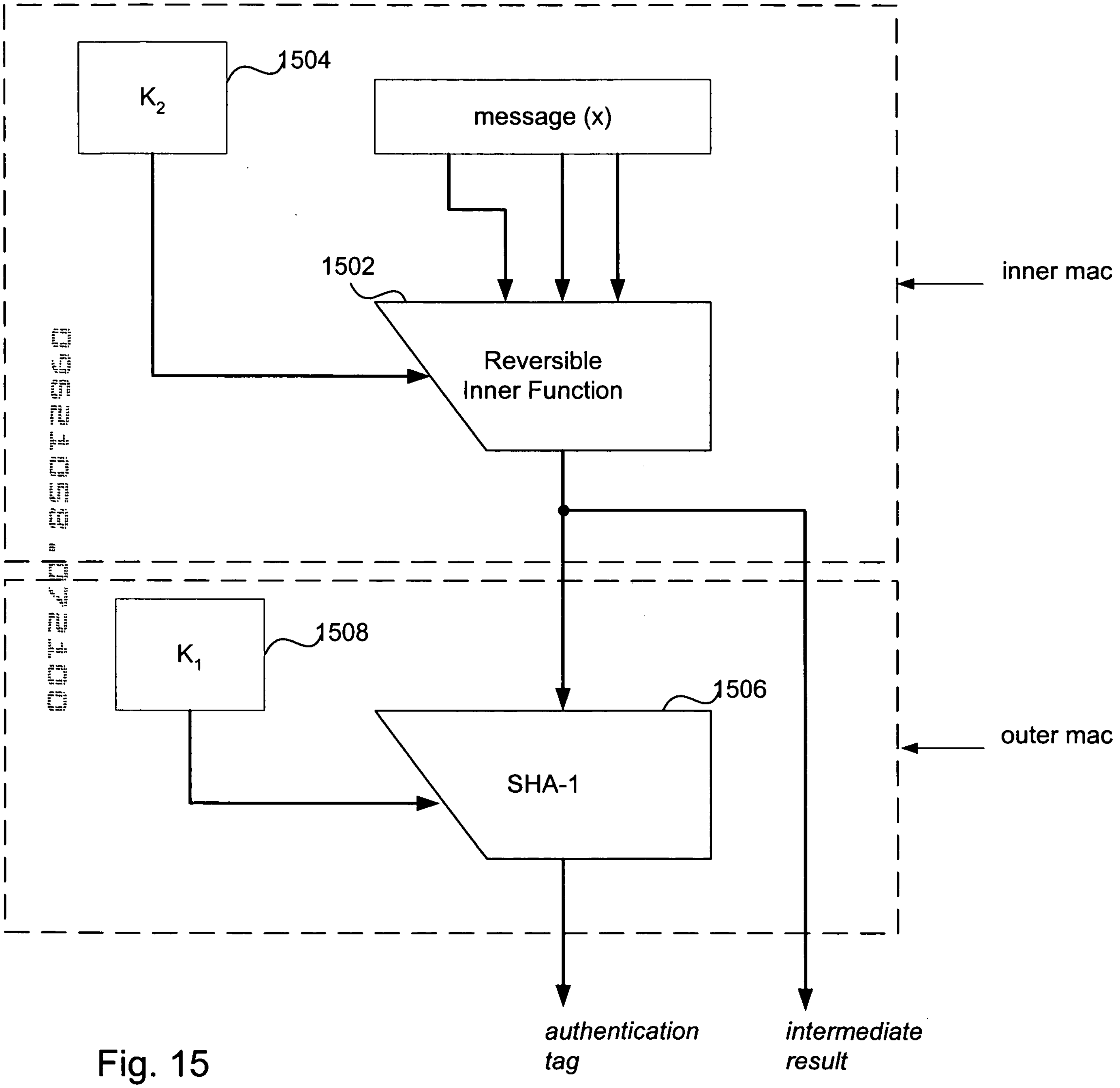

K$_2$
1504
message (x)
1502
Reversible Inner Function
inner mac
K$_1$
1508
1506
SHA-1
outer mac
authentication tag
intermediate result

Fig. 15

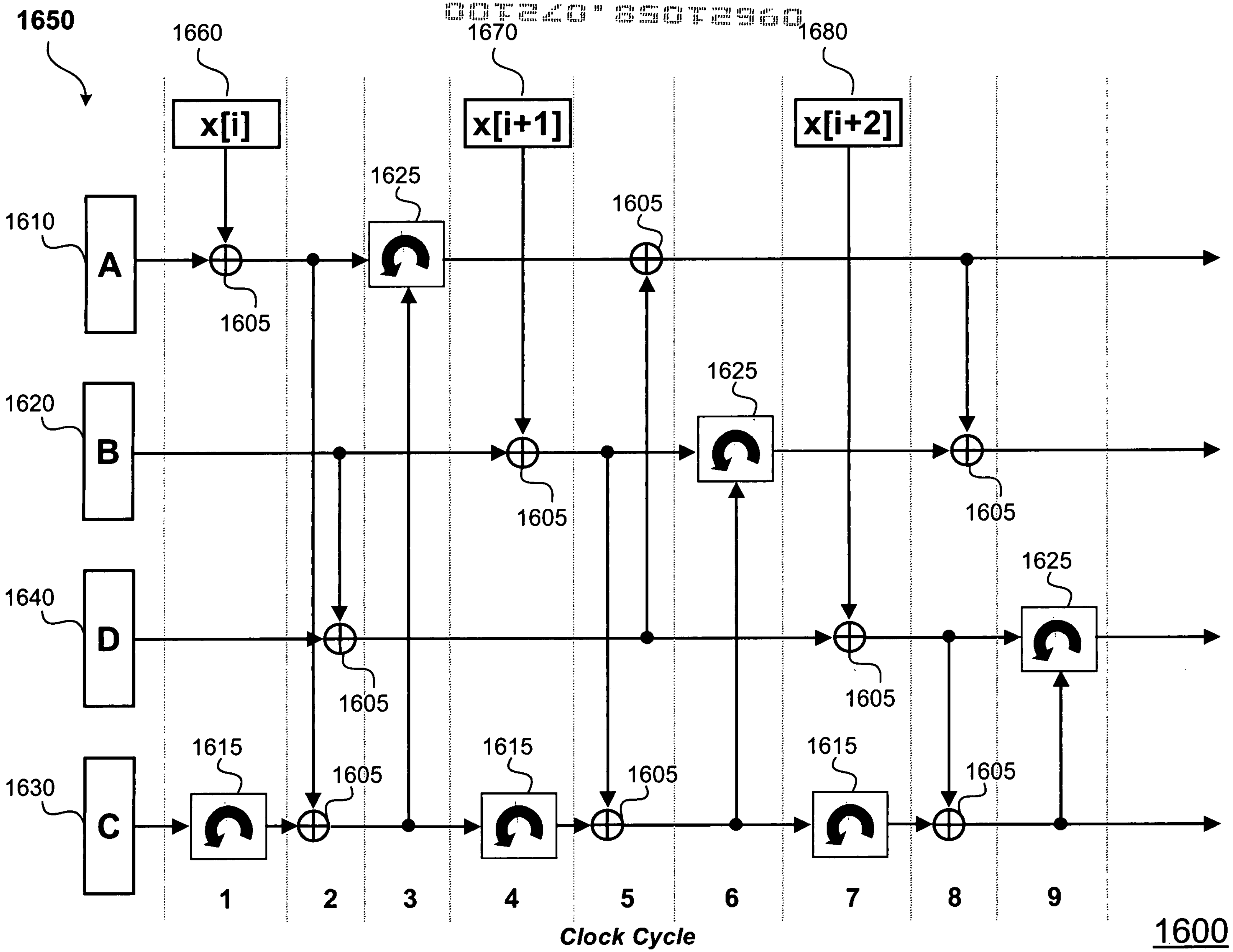

1650
1660
x[i]
1670
x[i+1]
1680
x[i+2]
1610
A
1620
B
1640
D
1630
C
1605
1615
1625
1
2
3
4
5
6
7
8
9
Clock Cycle
1600

FIG. 16

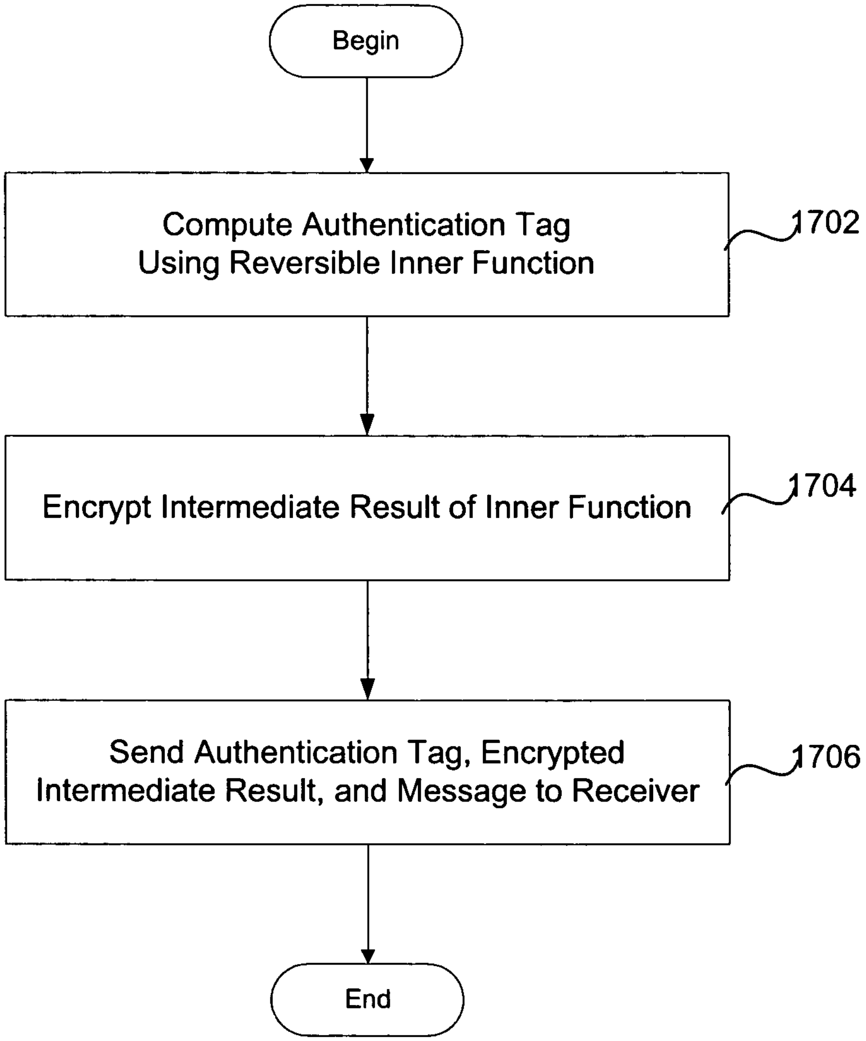

Begin
Compute Authentication Tag Using Reversible Inner Function
1702
Encrypt Intermediate Result of Inner Function
1704
Send Authentication Tag, Encrypted Intermediate Result, and Message to Receiver
1706
End

FIG. 17A

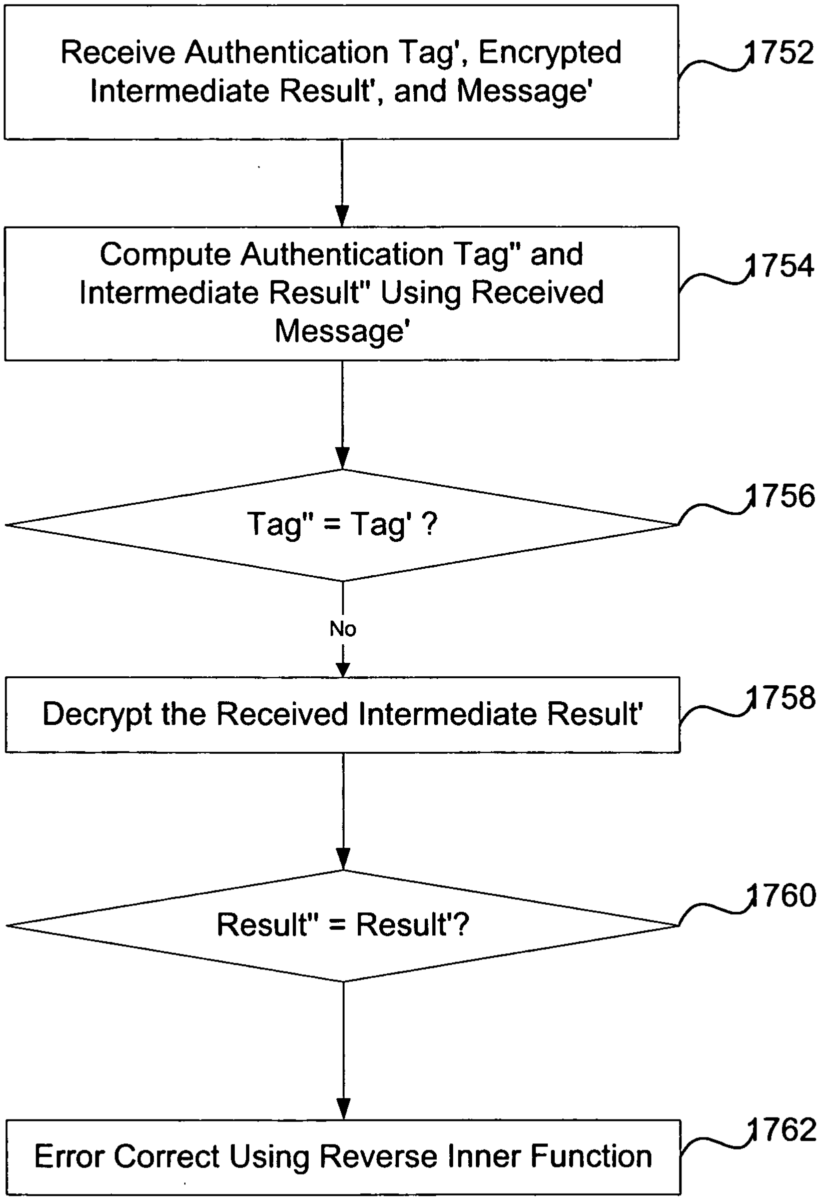

Receive Authentication Tag', Encrypted Intermediate Result', and Message'
1752
Compute Authentication Tag" and Intermediate Result" Using Received Message'
1754
Tag" = Tag' ?
1756
No
Decrypt the Received Intermediate Result'
1758
Result" = Result'?
1760
Error Correct Using Reverse Inner Function
1762

FIG. 17B